

From: "Dinesh Maneyapanda" <DManeyapanda@princeton.com>
To: key-recovery@nist.gov
Date: Mon, 15 Nov 1999 09:55:51 -0500
Subject: key escrow

Notwithstanding concerns about data encryption being used in the furtherance of the commission of crime, key escrow is a ridiculously stupid answer to the question.

First of all, high-bit encryption which does not use key escrow can be easily found outside the US for those criminals who plan to use it to help commit crimes. You need to recognize that the US and its laws are not the limiting factors in technology regulation any more.

Second of all, it is the nature of checks and balances that the enforcement arms of executive branches of government constantly try to push the envelope of acceptable behavior. You're kidding yourself if you think I'll trust my encrypted communication to that group's honesty and integrity, or even to a government-sanctioned third party who ultimately has to bow down to pressure from that same group.

Don't make the mistake of pushing key escrow. Clearly, public opinion is against it. Unbreakable encryption will just become merely another product we can get better and more cheaply from foreign sources.

Dinesh Maneyapanda